Next Generation Network and Reliability

Authors Pertti Raatikainen

Confidentiality Public

Report's title Next Generation Network and Reliability	
Customer, contact person, address	Order reference
Project name IPLU	Project number/Short name
Author(s) Pertti Raatikainen	Pages 15
Keywords next generation network, reliability	Report identification code VTT-R-
Summary	
Confidentiality	Public
Espoo, 10.1.2007 Signatures	
VTT's contact address Vuorimiehentie 3, Espoo, PL 1000, 02044-VTT	
Distribution (customer and VTT)	

The use of the name of the Technical Research Centre of Finland (VTT) in advertising or publication in part of this report is only permissible with written authorisation from the Technical Research Centre of Finland.

Preface

This report has been produced as part of the IPLU (Dependability of All IP Networks) project to give a short introduction to ITU-T's NGN network concept and to discuss reliability of the NGN networks. The discussion bases on the work carried out in the IPLU project.

Contents

Acronyms

ANI	Application-to-Network Interface
AS	Application Server
BGCF	Breakout Gateway Control Function
CSCF	Call Session Control Functions
DDOS	Distributed Denial of Service
DNS	Domain Name Service
DSCP	Differentiated Services field Code Points
DSL	Digital Subscriber Line
ENUM	Telephone Number Mapping
HSS	Home Subscriber Server
I-CSCF	Interrogating Call Session Control Functions
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
ISDN	Integrate Services Digital Network
ISUP	Integrated Service Digital Network User Part
MGCF	Media Gateway Control Function
MGW	Media Gateway
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
NAPT	Network Address and Port Translation
NNI	Network-Network-Interface
NGN	Next Generation Network
QoS	Quality of Service
P-CSCF	Proxy Call Session Control Functions
PSTN	Public Switched Telephone Network
RACF	Resource and admission control functions
RTP	Real-Time Transport Protocol
S-CSCF	Serving Call Session Control Functions
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
UE	User Equipment
UNI	User-to-Network Interface
W-CDMA	Wideband Code-Division Multiple Access
3GPP	3rd Generation Partnership Project

1 Introduction to NGN

The Next Generation Network (NGN) concept defines telecommunications network architectures and technologies. It describes networks that cover conventional PSTN (Public Switched Telephone Network) type of data and voice communications as well as new types of service such as video. All information is carried in packet switched form, as is done in the Internet. Packets are labelled according to their type (data, voice, video, etc) and forwarded in the network based on their Quality of Service (QoS) and security parameters.

The NGN makes a clear separation between the transport and services [1], which is advertised to allow smooth introduction of new services. When a provider wants to launch a new service, the service is defined directly at the service layer without considering the transport layer, i.e. services are independent of the transport technology [5][8].

1.1 NGN architecture

Due to the separation of transport and services, the NGN functions are divided into service and transport layers [2]. End-user functions are connected to the NGN by the user-to-network interface (UNI), while networks are interconnected via the network-to-network interface (NNI). The application-to-network interface (ANI) is defined to allow third-party application implementations. Figure 1 illustrates the overview of the NGN functional architecture.

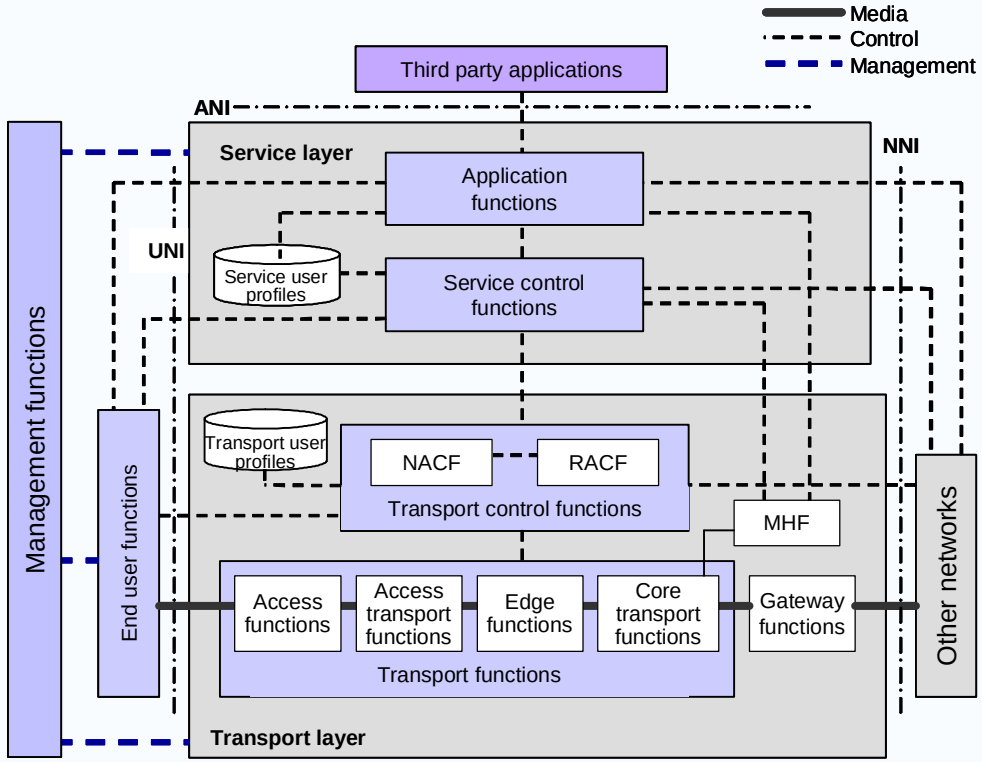

Figure 1. Overview of NGN functional architecture. [7]

1.2 Transport functions

The transport layer functions provide connectivity for all components and physically separated functions within an NGN. Internet Protocol (IP) is seen as the most obvious NGN transport technology and therefore the transport layer will provide IP connectivity for end-user equipment (residing outside an NGN) and various controllers and enablers that are usually located in servers within the area of an NGN. The transport layer is further divided into access and core network. The following lists the major transport functions (see Fig. 1) [2][7]:

Access functions, which are access technology dependent, manage the end-user access to an NGN network. Access technologies, such as cable access, DSL, wireless technology, Ethernet technology and optical access, are supported.

Access transport functions are responsible for carrying information across the access network. They also offer QoS control mechanisms that deal directly with user traffic, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing and traffic shaping.

Edge functions are used for traffic processing when access traffic is merged into the core network.

Core transport functions ensure information transport through the core network. They provide the means to differentiate the quality of transport by interacting with the transport control functions. Additionally, they offer QoS mechanisms to control directly user traffic, e.g. by means of buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing and shaping, gate control and firewalls.

Network attachment control functions (NACF) provide registration at the access level and initialisation of end-user functions to allow access to NGN services. They support network-level identification and authentication, manage the IP address space of the access network, and authenticate access sessions. They also announce the contact point of the NGN service and application functions to the end-user, thus assisting the end-user equipment in registering and starting to use the NGN.

Resource and admission control functions (RACFs) offer admission control and gate control functionality, such as control of network address and port translation (NAPT) and management of differentiated services field code points (DSCPs). Admission control includes, e.g. user profile based checking of authentication and authorisation, considering also operator-specific policy rules and resource availability. Resource availability checking implies that the admission control function verifies whether a resource request (e.g., for bandwidth) is allowable, as opposed to resources that are already provisioned or used. The RACFs interact with transport functions to control one or more of the following transport layer functions: packet filtering, traffic classification, marking and policing, bandwidth reservation and allocation, NAPT, anti-spoofing of IP addresses and usage metering.

Transport user profile functions comprise the user and other control information that form a single “user profile” function in the transport layer. This function may be specified and implemented as a set of cooperating databases with functionality residing in any part of an NGN.

Gateway functions support capabilities to interwork with other networks, such as PSTN/ ISDN-based networks and the Internet. Interworking with other NGNs, owned and operated by other administrators, is also included.

Media handling functions (MHF) supply services, such as tone signal generation, transcoding and conference-call bridging.

1.3 Service functions

NGN services will include session-based and non-session-based services. Examples of the session-based services are IP telephony and video conferencing, and examples of the non-session-based services are video streaming and broadcasting. The NGN supports also network functionality associated with existing PSTN/ISDN services and capabilities and interfaces to legacy customer equipment. [2][6][7]

Service and control functions include session control functions, a registration function as well as authentication and authorization functions at the service level.

Service user profile functions cover the user and other control information that form a single user profile function in the service layer. The function may be specified and implemented as a set of cooperating databases with functionality located in any part of an NGN.

Application functions, either trusted or untrusted, are used by third-party service providers to access NGN service layer capabilities and resources through servers or gateways in the service layer. These functions are needed, because NGNs support open APIs that enable third-party service providers to use NGN capabilities in creating enhanced services for NGN users.

1.4 Management functions

The management functions enable an NGN operator to manage the network and provide NGN services with the required quality, security and reliability. These functions are distributed to each functional entity and they interact with the network element management, network management and service management functional entities. [7][9]

The management functions include charging and billing functions, which interact with each other to collect resource utilisation information. This information enables the operator to bill users properly. The collected charging and billing information can be used for online interactions, such as for prepaid services, and for offline interactions.

1.5 End-user functions

Interfaces to the end-user are either physical or functional (control) interfaces, as shown in Figure 1. The ITU-T specifications do not limit the types of customer interface that can be connected to an NGN network. The NGN supports all kinds of customer equipment categories from single line legacy telephones to complex corporate networks. Additionally, the end-user equipment may be either mobile or fixed. [1][7]

1.6 IP multimedia subsystem (IMS)

The IP Multimedia Subsystem (IMS) has a central role in providing session based services for the NGN. IMS is based on IP protocols defined by Internet Engineering Task Force (IETF). The 3rd Generation Partnership Project (3GPP) defined IMS for mobile networks and it was also introduced for the NGN. IMS is mostly independent of the access network technology, although there are some transport specific aspects. The basic signalling protocol used by IMS is the Session Initiation Protocol (SIP), which is used to create, modify and terminate sessions. [3][4][9]

IMS architecture

IMS makes separation between the core and access network. The separation comes from 3GPP's original IMS definitions, i.e. from the wireless network model in which one or more radio access networks are connected to a common core network [4]. The radio access networks provide connections between terminals and services available in the core. An access network is a collection of entities providing IP transport connectivity between a user domain and a core transport network. Different sorts of access networks are distinguished based on the underlying technology, ownership or administrative partitioning.

IMS defines a collection of core network functional entities that the core uses in offering IP transport connectivity between an access network and a core transport network, between two access networks or between two core networks. The core network also offers connectivity to service layer entities. The core networks can differ from one another according to the underlying technology, ownership or administrative partitioning.

One of the fundamental characteristics of an IMS is the support of user mobility. In this context, the distinction between the core and access networks has significance, especially when dividing the functions necessary to support an IMS. Figure 2 illustrates how an NGN network is composed of access, core and transit networks. A user can move from an access network to another and access to the originating core network's services is maintained.

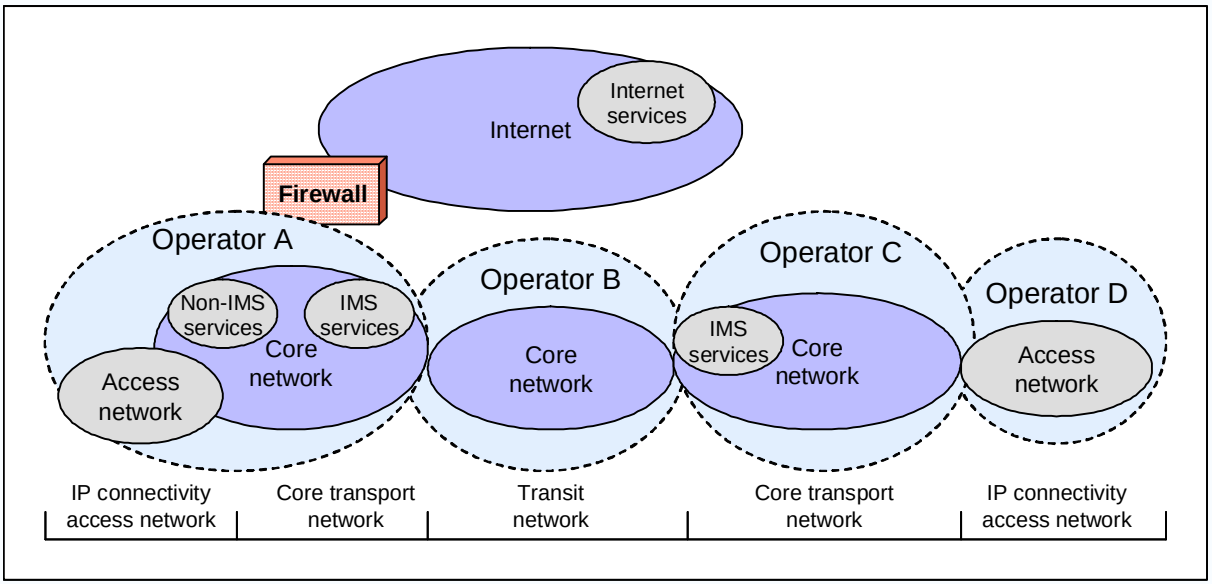

Figure 2. Network partitioning in respect of IMS. [7]

IMS Functional Entities

Figure 3 shows the collection of functional entities and reference points of the IMS functional architecture. The purpose of each entity is explained shortly in the following.

An **application server** (AS) provides service control for the IMS. The AS may be directly connected to a serving call session control function (S-CSCF) or via an Open Services Architecture (OSA) gateway for third-party based applications over an *ISC* reference point. The ISC interface is SIP-based and SIP messages may be carried over this interface to or from an S-CSCF. The AS may interact with the home subscriber server (HSS) over the *Sh* interface to obtain subscriber profile information. Application servers are used to support various telephony-type services, e.g. call forwarding and number translation, and they may also support such services as presence, conference control and online charging.

A **breakout gateway control function** (BGCF) receives session requests forwarded by an S-CSCF (or another BGCF) and selects the network in which a PSTN attachment point is located. It also selects a local MGCF or a peer BGCF in another network. The ability to select a BGCF in another network enables to optimise routing from a visited network to the PSTN.

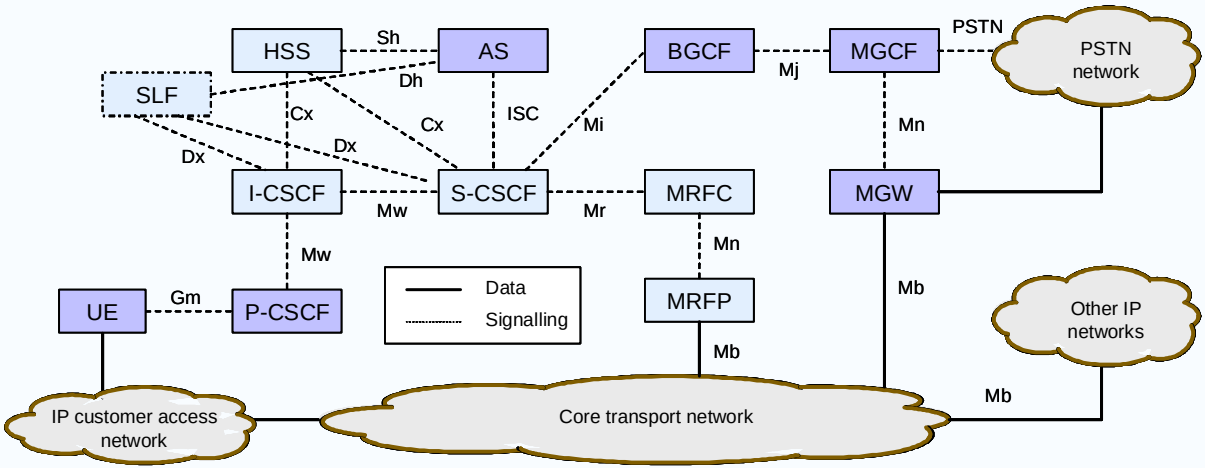

Figure 3. IMS functional entities and reference points.

Call Session Control Functions (CSCF) are responsible for the control of session features, routing and resource allocation in cooperation with other network elements. When a SIP enabled terminal initiates a call, CSCF allocates resources and routes the SIP invite message to the called terminal. If the called side is a traditional PSTN phone number then CSCF routes SIP messages to the Breakout Gateway Control Function (BGCF). BGCF selects the Media Gateway Control Function (MGCF), which perform necessary signalling conversion.

The IMS architecture supports three types of CSCFs: Serving CSCF (S-CSCF), Interrogating CSCF (I-CSCF) and Proxy CSCF (P-CSCF).

S-CSCF acts as a registering function [3]. It accepts SIP *register* requests and creates a binding between the public user ID and the terminal location. S-CSCF retrieves the subscriber profile from the HSS, including filter criteria that indicate the ASs that offer service control to this user. To support service control, the S-CSCF interacts with these ASs during the SIP

signalling. During a session establishment or modification phase, the S-CSCF monitors the Session Description Protocol (SDP) to ensure that the session is within the boundaries of the subscriber's profile.

The S-CSCF also performs routing of SIP messages on behalf of the originating user equipment (UE). It obtains the address of an I-CSCF (or another IP endpoint) from a domain name server (DNS) by using the destination name of the terminating subscriber. After that it forwards the SIP request toward the destination. If the destination name of the terminating subscriber is a PSTN address, the S-CSCF forwards the request to a BGCF for routing toward the PSTN. On behalf of the destination endpoint, the S-CSCF forwards the SIP request to a P-CSCF according to the subscriber's registered location, or for an unregistered subscriber it may send or redirect the SIP request to an alternate endpoint.

I-CSCF serves as the initial point of contact to the IMS home network from other networks. It performs a stateless SIP proxy function and directs received SIP requests to S-CSCF, assigned to the user, or selects an S-CSCF if one is not currently assigned. I-CSCF assigns SCSCFs upon initial UE registration and when terminating services for unregistered users.

P-CSCF serves as the initial point of contact for a user terminal to the IMS. It performs a stateful SIP proxy function by sending SIP *register* requests from the UE to an I-CSCF, which resides in the home network. The home network is determined by using the home domain name, provided by the UE. The P-CSCF sends all subsequent SIP messages, received from the UE, to the S-CSCF whose name it has received during the registration procedure. The P-CSCF also ensures that a valid public user identity of the IMS user is inserted into UE-initiated SIP requests.

Home Subscriber Server (HSS) contains a subscription database for the IMS. It supports IMS-level authentication and authorization as well as keeps record of the IMS subscriber profiles. The HSS also stores the currently assigned S-CSCF. A home network may contain one or several HSSs. The number of HSSs depends on the number of subscribers, the capacity of the equipment and the organization of the network.

Media Gateway Control Function (MGCF) supports interworking between the IMS and the PSTN. MGCF performs the translation between SIP messages and Integrated Service Digital Network User Part (ISUP) messages. MGCF also controls MGW.

Media Gateway (MGW) terminates bearer channels from circuit-switched networks and media streams from packet switched networks and performs media conversion functions such as transcoding. It also offers dual tone multi-frequency (DTMF) detection and generation.

Media Resource Function Controller (MRFC) controls MRFP's media stream resources. It interprets information from an AS or SIP endpoint and controls the MRFP accordingly to support media services such as transcoding and conferencing. The MRFC may be co-located with an AS to support specialised AS services.

Media Resource Function Processor (MRFP) supports functions such as media stream mixing, tone and announcement generation, transcoding and media analysis.

Subscription Locator Function (SLF) acts as a front-end for distributed HSS systems. It may be queried by an I-CSCF during registration and session setup to get the name of the HSS, which contains the required subscriber-specific data. The SLF may also be queried by the S-CSCF during registration or by the AS in connection with the *Sh* interface. The SLF is not needed in a single-HSS environment or in certain other HSS environments, such as a server-farm architecture.

User Equipment (UE) represents the functionality of user terminals. It supports the specific capabilities of the access network to which it is connected. It also supports the user agent capabilities of an IMS client. The UE supports SIP methods/functions as defined by the IMS.

2 NGN reliability

The NGNs are going to be a mixture of circuit and packet switched networks and technologies, for which reason it is not easy to say whether the reliability of an NGN network is closer to that of a conventional PSTN network or the Internet. The following discusses some of the concerns as well as improvements that make the NGN concept more reliable than the Internet.

2.1 Performance concerns

As stated in chapter 1, NGNs are based on the Internet technology, which means that the NGNs are basically subject to the same dependability concerns as the native IP networks. There are several matters that cause concern, e.g.

- open and distributed nature
- lack of inherent security mechanisms
- increasingly complicated network concept
- running of mission-critical applications
- deployed before fully matured
- few expert solutions for effective management
- require time- and cost-consuming integration and configuration

The open architecture implies that any company or any person can develop applications for the NGN and run them on an NGN network. Thus it will become difficult to prepare for possible malicious applications, either end-user or control applications. The distributed nature, in turn, implies that it is difficult to locate and eliminate the observed disturbances, especially in cases when the disturbance is able to move in the network and/or make copies of itself to various locations of the network. Therefore, the avoidance of disturbing applications is going to be more reactive than proactive.

Inherently secure PSTN functions are modified to adapt to the packet switching paradigm, which often degrades the security of communication. An example is the numbering scheme (E.164) that needs to be modified to allow the internet type of addressing mechanism. The new telephone number mapping (ENUM) scheme builds on the Internet's domain name server system (DNS) introducing similar performance problems as present in the DNS system. Examples of such problems are the distributed denial of service (DDOS) and DNS pollution problems.

Mission-critical applications, such as banking, medical systems and power station control, require error-free transport, short response times and absolute security. The Internet type of data transport does not guarantee delivery of IP packets to their intended destinations. Packets may be dropped, delayed or directed to false destinations. The more load in the network the

more obvious it becomes that packets are dropped or delayed. Spoofing is a known problem in conventional IP networks and the NGN's open architecture preserves that problem. The spoofing term stands for the various techniques that enable unauthorised access to computers and user information. Examples of the spoofing techniques are the man-in-the-middle, source routing and flooding.

In the conventional circuit switched networks, redundancy has been used to guarantee performance of the critical network functionality. In the packet switched networks, there has been a habit to manage with the lowest cost, i.e. redundancy is seldom used to guarantee even the critical functionality. Since the NGN networks are supposed to replace the old established telecom infrastructure, attention has to be paid on reliability and availability of the network functions even if it means additional cost. Carrier-grade transport assumes, e.g. that agreed availability measures are fulfilled. Redundant links, network devices and software modules offer a practicable way to provide required reliability.

Benefits of the packet based technology are advertised to be so crucial to lucrative telecommunications business that networking companies are willing to implement new technology before standardisation is complete and there is enough information on implementation problems. Too hasty adaptation of the all-IP solutions also means that there are no efficient network management solutions available to ease the implementation of the new technology. The integration of conventional network technology with the all-IP technology no doubt increases complexity. Therefore, implementation of new solutions to run smoothly with the conventional technology is going to be time-consuming and costly. Furthermore, there is a lack of trained professionals to deal with the new technology and its problems.

Provided that the essential control and management connections and devices are adequately protected and redundant units implemented, the performance and security threats may be lowered substantially. It is to be seen whether the NGN concept is able to give sufficient implementation directions to allow product manufactures and network operators to build coherent and secure networks. However, it is difficult to see, how the NGNs will ever reach the same level of performance reliability as the old established PSTNs used to have.

2.2 Enhanced internet quality

Although the NGN utilises the same technology as the Internet, there are additions that make the NGN at least a slightly different from the Internet. The main difference is the IMS, which builds on the IETF protocols, but implements specific profiles and enhancements to provide a robust multimedia system. The enhancements and operational profiles offer support for operator control, billing and security. Additionally, IMS requires a set of vertical interfaces to provide the following:

- common interfaces to application servers for accounting, security, subscription data, service control and to service building blocks
- coordinated and enforced QoS (session layer negotiation can be matched with resources granted at the transport layer, per operator policy)
- session-based media gating under operator control
- correlated accounting and charging among the service, session and transport layers

The above capabilities make IMS and thus the NGN different from the Internet on session control point of view. A network operator controls access to the network and a service provider controls access to the services. This feature is contradictory to the usual Internet model in which the network is transparent and all services are provided by endpoints. Users get an improved experience with managed QoS, single sign-on security and customer support, at least in theory. Thus it can be concluded that the NGN, despite of its complex structure, is more controllable and therefore more reliable than the usual Internet.

References

[1] ITU-T Rec. Y.2001, “General Overview of NGN”.

[2] ITU-T, Rec. Y.2011, “General Principles and General Reference Model for Next Generation Networks”.

[3] IETF RFC3261, “SIP: Session Initiation Protocol”.

[4] 3GPP IP Multimedia Subsystem Release 6, TS 23.228.

[5] C.-S. Lee, D. Knigth, “Realization of the Next-Generation Network”, IEEE Communications Magazine, Oct. 2005, pp 34-41.

[6] N. Carugi, B. Hirschman, A. Narita, “Introduction to the ITU-T NGN Focus Group Release 1: Target Environment, Services, and Capabilities”, IEEE Communications Magazine, Oct. 2005, pp. 42-48.

[7] K. Knightson, N. Motita, T. Towle, “NGN Architecture: General Principles, Functional Architecture, and Implementarion”, IEEE Communications Magazine, Oct. 2005, pp. 49-56.

[8] V. K Gurbani, X.-H. Sun, A. Brusilovsky, ”Inhibitors for Ubiquitous Deployment of Services in the Next-Generation Network”, IEEE Communications Magazine, Sept. 2005, pp. 116-121.

[9] A. R. Modarresi, S. Mohan, “Control and Management in Next-Generation Networks: Challenges and Opportunities”, IEEE Communications Magazine, Oct. 2000, pp. 94-102.